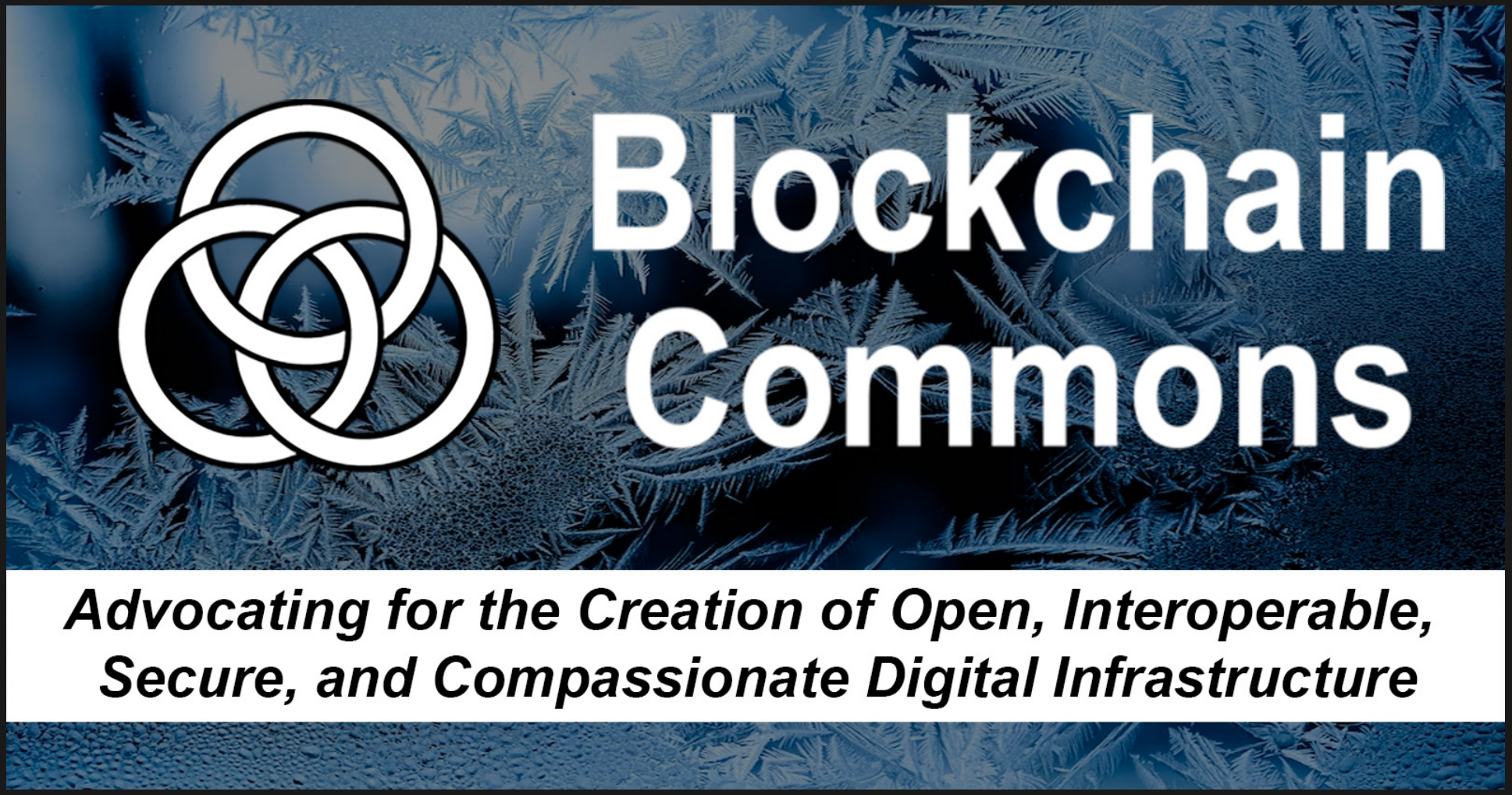
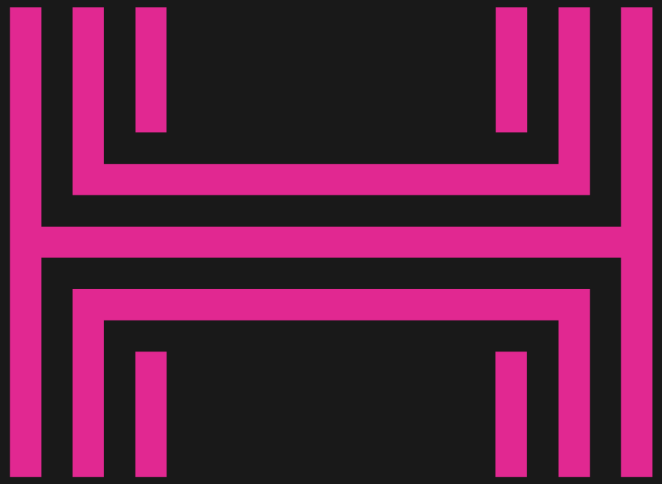


FROST CLI #Gordian Meeting 9/6/25

What is Blockchain Commons?

- We are a community interested in self-sovereign control of digital assets.
- We bring together stakeholders to collaboratively develop interoperable infrastructure.
- We design decentralized solutions where everyone wins.
- We are a neutral "not-for-profit" that enables people to control their own digital destiny.

Thank you to our FROST Sponsor!



Human Rights Foundation

Become a sponsor! Mail us at team@blockchaincommons.com

Two Great Tools

- We've been working with two great tools
- ZF FROST
  - https://frost.zfnd.org/
- Bitcoin Dev Kit (BDK)
  - https://bitcoindevkit.org/

🧩 Our Biggest Puzzle

- How Do We combine ZF FROST & BDK for PSBT Signing?
- ZF FROST Needed Secp256K1-TR Ciphersuite
- BDK Needed to Apply Signature
    - But Also Needed a "Tweak" to Avoid a Taproot Attack
        - Transaction hash must be extracted
        - Key Material is tweaked
        - Signature is reinserted

❄ ZF FROST

- We Built on Existing FROST CLI Tools
  - https://github.com/ZcashFoundation/frost-tools
- Submitted PR for Secp256K1-TR Ciphersuite
  - https://github.com/ZcashFoundation/frost-tools/pull/537
- Also have a branch which does Taproot tweak
  - https://github.com/BlockchainCommons/zcash-frost-tools/pull/2

🧰 BDK

- Extracting hash wasn't available in CLI.
- (Tweaking is an external process.)
- Reinserting signature wasn't available in CLI.
- Had to use libraries & write two tools to extract & reinsert sig
- But:
    - It's unclear who should be tweaking.
    - There may be privacy concerns for tweaking BIP-32 derivations.
    - Tweaking may not be necessary with FROST DKG.
    - More on this all after our demo!

Blockchain Commons Demo

- Demo:
  - Spend Taproot (P2TR) Bitcoin
  - On a private regtest network
  - Using a 2-of-3 FROST signature
- We will:
  - Create 3 keyshares with Trusted Dealer
  - Create a PSBT
  - Run `sighash-helper` to get Taproot key-path sighash
  - Sign with FROST
  - Inject signature with `psbt-sig-attach`
  - Transmit!
- Over to Wolf!

❄️ ZF FROST DKG Open Questions

- We were unable to get the ZF Distributed Key Generation (DKG) server to work, it may be a few steps behind the TD (Trusted Dealer) code.
- There doesn't seem to be any standards for the DKG values. I don't believe any of the three DKGs we've tested can be used with a different FROST signing system.

❄ ZF FROST Open Questions

On PRs:

- What is the status of PRs to ZF FROST?
- Does DKG make that Taproot tweak unnecessary?
- Does it make sense to submit tweak PR?
- Do we need to add optionality to tweak PR?

On Reviews:

- Did Schnorr BIP340 get security reviewed?
- Will Zcash be doing more security reviews?

🧰 BDK Open Questions

- Should BDK expose retrieving hash?
- SHould BDK expose re-inserting signature?
- Who would we talk to to make this happen?
- What if there is no requirement for tweak?
    - (e.g., with FROST DKG)

🔮 Other Open Questions

- Which party is really responsible for applying the Taproot tweak?
- What should be done when it's not required?
- Can we make the tweak more private by doing it at a different place?

❄️ FROST is Coming!

- We have a variety of resources and results from previous FROST workshops at: https://developer.blockchaincommons.com/frost/
- We will have more focused FROST meetings this fall.
- If you'd like to present, let us know!
    - ***Library Implementers:*** Tell us about your tech and roadmap
    - ***Developers:*** Tell us about your needs and use cases

www.BlockchainCommons.com

Christopher Allen (@ChristopherA)